

BEST AVAILABLE COPY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-282672

(43)Date of publication of application : 15.10.1999

(51)Int.CI.

G06F 9/06

(21)Application number : 10-084836

(71)Applicant : HITACHI SOFTWARE ENG CO LTD

(22)Date of filing : 31.03.1998

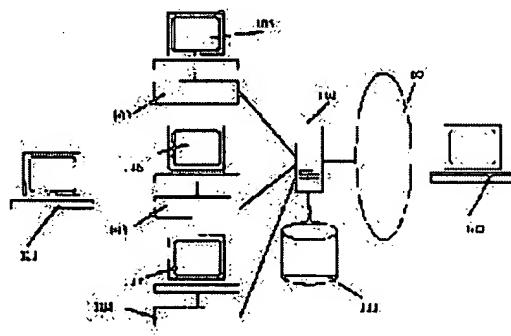
(72)Inventor : KONDO MARIKO
TAGO SHIGERU

(54) TRANSFER METHOD AND EXECUTION SYSTEM FOR ON-LINE PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To directly prove that a program which is transferred on line has no dangerous operation by giving an electronic signature to the program when it's distributed via an inspector and confirming the signature to permit the execution of the transferred program before it's executed.

SOLUTION: A program producer produces programs via a program developing device 101, and the programs are copied and transferred to the program execution systems 105 to 107. The users (inspectors) of systems 105 to 107 execute the transferred programs to check whether the programs have dangerous operations. When it's confirmed that a function group to be inspected has no dangerous operation, the electronic signatures are given to the programs via the electronic signature devices 102 to 104. A program transmission request is given to a server system 110 from a program execution system 108 after the inspection, and the system 110 sends the data to the system 108.



LEGAL STATUS

[Date of request for examination] 23.06.2000

[Date of sending the examiner's decision of rejection] 12.08.2002

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C) 1998,2003 Japan Patent Office

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-282672

(43)公開日 平成11年(1999)10月15日

(51)Int.Cl.⁶
G 0 6 F 9/06

識別記号
5 5 0

F I
G 0 6 F 9/06

5 5 0 Z

審査請求 未請求 請求項の数7 O L (全 8 頁)

(21)出願番号 特願平10-84836

(22)出願日 平成10年(1998) 3月31日

(71)出願人 000233055

日立ソフトウェアエンジニアリング株式会
社

神奈川県横浜市中区尾上町6丁目81番地

(72)発明者 近藤 麻里子

神奈川県横浜市中区尾上町6丁目81番地
日立ソフトウェアエンジニアリング株式会
社内

(72)発明者 多胡 滋

神奈川県横浜市中区尾上町6丁目81番地
日立ソフトウェアエンジニアリング株式会
社内

(74)代理人 弁理士 秋田 収喜

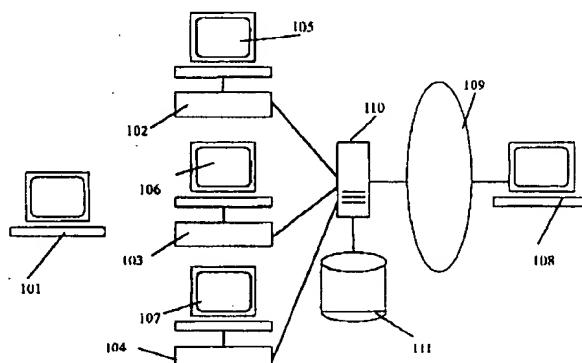
(54)【発明の名称】 オンラインプログラム転送方法およびオンラインプログラム実行システム

(57)【要約】

【課題】 プログラム開発者とは別に、そのプログラムが不正な動作をしないことをチェックし、電子署名を施す第3者(検証者)を用意することで、認証手続きを簡略化する。

【解決手段】 プログラムを計算機外部から計算機内部に転送するに先立ち、該プログラムの作成者以外の特定の人あるいは組織により、該プログラムを該プログラムの全体あるいは一部に、起動した人あるいは組織が認識不可能な動作をしないことを保証する電子署名を施し、該プログラムを起動する人あるいは組織による確認が行わされた後に当該プログラムを計算機内部に転送する。

図1



【特許請求の範囲】

【請求項1】 オンラインで計算機内部に転送された後に起動されるプログラムの転送方法であって、前記プログラムを計算機外部から計算機内部に転送するに先立ち、該プログラムの作成者以外の特定の人あるいは組織により、該プログラムを該プログラムの全体あるいは一部に、起動した人あるいは組織が認識不可能な動作をしないことを保証する電子署名を施し、該プログラムを起動する人あるいは組織による確認が行われた後に当該プログラムを計算機内部に転送することを特徴とするオンラインプログラム転送方法。

【請求項2】 前記電子署名を、前記プログラムの機能グループごとに異なる複数の人あるいは組織により施すことを特徴とする請求項1記載のオンラインプログラム転送方法。

【請求項3】 オンラインでプログラムを受信の後、該プログラムを演算処理装置上で実行するプログラム実行システムにおいて、

該プログラムの作成者以外の特定の人あるいは組織により、該プログラムの全体あるいは一部に電子署名が施されており、かつ該電子署名が確認された場合にのみ、該プログラムの実行を許可する手段を備えることを特徴とするオンラインプログラム実行システム。

【請求項4】 前記プログラムが有する機能グループのいずれに電子署名が施されているかを調べ、機能グループのいずれの実行を許可するかを変更する手段を備えることを特徴とする請求項3記載のオンラインプログラム実行システム。

【請求項5】 オンラインでプログラムを受信後、該プログラムを演算処理装置上で実行するプログラム実行システムにおいて、

複数の実行可能な機能の実行の許可あるいは不許可を、プログラム別および機能別に記憶する手段と、特定の機能を実行する直前に、該機能の実行の許可あるいは不許可を実行者に選択させる手段と、許可されている機能を実行させ、許可されていない機能を実行させない手段とを備えることを特徴とするオンラインプログラム実行システム。

【請求項6】 特定の機能を実行する直前に、該機能の詳細を実行者に示し、その機能の実行が実行者にとって不利益とならないことを実行者自身に確認させる手段を備えることを特徴とする請求項5記載のオンラインプログラム実行システム。

【請求項7】 複数の機能の許可あるいは不許可を、プログラム別および機能別に記録した設定データに対し、該設定データの作成者が電子署名を施す機能と、該設定データに対する該電子署名を確認する手段と、特定の設定データ作成者に対し、その作成者が作成した設定データの内容を取り込み、該プログラムの実行に当たって各機能の実行の許可あるいは不許可を該設定データに従つ

10

20

30

40

50

て決定する手段を備え、あるプログラム実行システムにおいて設定された機能別の実行の許可あるいは不許可の設定を、その作成者による電子署名が確認された場合に、同一の、あるいは別のプログラム実行システムにおいて適用することを特徴とする請求項5または6記載のオンラインプログラム実行システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、オンラインでプログラムを受信の後、そのプログラムを実行する機能を備えた計算機などのオンラインプログラム実行システムおよびそのオンラインプログラムの転送方法に関するものである。

【0002】

【従来の技術】 ある計算機上でプログラムを実行する場合、そのプログラムを、予めその計算機に接続された補助記憶装置上に記憶しておき、実行時に読み出すことによって実行する方式が最も一般的であるが、一方で、プログラムはオンラインに接続されたサーバシステムの補助記憶装置上に記憶しておき、実行時に、オンライン経由でプログラムを計算機上に転送し、実行するという方法が多く利用されるようになっている。

【0003】 しかし、この方法では、利用者が該当するプログラムの実行開始を明示的に指示しない場合が多く、もしそのプログラムが利用者にとって不利益になるような動作をするものであったとしてもその動作を行う前に実行を中断する手段がない場合がある。

【0004】 このような危険を避けるため、該当するプログラムの全体あるいは一部に対して、そのプログラムの作成者が電子署名を施すことにより、利用者に対してプログラムが確かにその作成者によって作成されたものであり、他者によって改ざんされていないことを証明し、危険な動作をしないことを保証しようとする方法が主に用いられている。

【0005】

【発明が解決しようとする課題】 しかし、上述の従来の方法では、次のような問題がある。

【0006】 1) 作成者が本人であることは証明できるが、そのプログラムが危険な動作をしないことを直接的には証明できない。危険な動作とは、利用者の許可なしに、ファイルのロックを解除する、ファイルを更新する、認証を与える、プログラムを更新するなど、利用者本人にとって不利益をもたらす動作、あるいはもたらすかも知れない動作のことである。従来は、作成者の組織名等を見て、信用する、しないを各利用者が適宜判断することで運用していた。

【0007】 2) 多数のプログラムを実行させる場合、それらの作成者として多くの人あるいは組織を信用するようプログラム実行システムに設定する必要があり、作業が煩雑であり、また、信用度の検討が疎かになるとい

う弊害がある。

【0008】3) 危険な動作をするか、しないかの2者
選一設定であるため、ある機能については危険な動作を
しないプログラムであったとしても、別の機能について
保証できなければ、そのプログラム全体を信用すること
ができない。

【0009】4) 実行時のプログラム実行システムの環
境や、プログラムに入力されるパラメータによって、実
行者に不利益な結果を生む可能性がある。

【0010】5) 実行時のプログラム実行システムの環
境や、プログラムに入力されるパラメータによって、実
行者に不利益な結果を生む可能性がないにも関わらず、
一般的に不利益な結果を生む可能性があるという理由で
実行を許可されない場合がある。

【0011】本発明の第1の目的は、このような問題を
解決し、オンラインで転送されたプログラムが危険な動作
をしないことを直接的に証明することができるオンライン
プログラム転送方法およびオンラインプログラム実行
システムを提供することにある。

【0012】本発明の第2の目的は、実行者に不利益な
結果を生じさせないようにすることができるオンライン
プログラム実行システムを提供することにある。

【0013】

【課題を解決するための手段】上記目的を達成するため
に、本発明のオンラインプログラム転送方法は、まず、
プログラムの作成者とは別に、そのプログラムが危険な
動作をしないことを検証できる人あるいは組織を用意する。
プログラムの配布時に、この検証者によって電子署
名を施す。利用者は、転送したプログラムを実行する前
に電子署名を確認し、信用できる検証者によって電子署
名されているプログラムであった場合は、その実行を許
可する。

【0014】さらに、そのプログラムの機能グループ別
に検証者を用意し、その各々についての電子署名である
ことを明記した上で、プログラムに電子署名を施す。利
用者は、自分が利用したい機能についてのみ、電子署名
を確認し、その利用したい機能グループについて信用で
きる検証者によって電子署名されていた場合は、その機
能グループの実行を許可する。

【0015】また、上記第2の目的を達成するために、
本発明のオンラインプログラム実行システムは、特定の
プログラムをオンラインで受信後、実行する際に、複数
の機能に対してその実行直前に、実行者に対して、その
機能の実行を許可するかどうかを設定させる。

【0016】さらに、各機能の実行の許可を設定する時
点で、その機能の詳細を実行者に対して示すことによ
り、その機能の実行が実行者にとって不利益となるかど
うかを実行者自身が判断できるようにする。

【0017】そして、各機能に対する実行の許可／不許
可の設定を記憶し、以降、同プログラムの実行時には同
50

機能を前期設定に基づいて実行あるいは不実行を決定す
る。

【0018】また、記憶された各機能に対する実行の許
可／不許可の設定データに対し、そのデータの作成者が
電子署名を施し、そのデータの読み取り時に電子署名を
確認する。

【0019】

【発明の実施の形態】以下、本発明を図示する実施の形
態を参照して詳細に説明する。

第1の実施形態

図1は、本発明の第1の実施形態のシステム構成図である。
図1において、101は、本発明で対象としている
プログラムを作成するためのプログラム開発装置である。
102～104は、プログラムに対し電子署名を施す機能を持つ
電子署名装置、105～108は、プログラムを演算処理装置内で
実行する機能を持つプログラム実行システム、109は
プログラムの転送に使用するオンラインシステムである。
110は、オンライン経由でのプログラムの送信機能を持つ
サーバシステム、111はプログラムを記憶する機能をもつ
補助記憶装置である。

【0020】図2は、補助記憶装置111に記憶される
プログラムの構造を示している。図2において、201
は、プログラム実行システム105～108上で実行可能
なプログラム、202は、プログラム201に電子署
名を施した人あるいは組織の名前、203は、
プログラム201に電子署名を施した結果算出された
電子署名データ、204は、前記の名前202によって危険な動作
をしないことを保証された機能グループのID番号である。

【0021】図3はプログラム実行システム108において、
プログラム201を実行する前に設定するプログラム
実行許可設定データの構造を示している。図3において、
301は、プログラム201の機能グループのID番号、
302は、機能グループ301が危険な動作を
しないことを電子署名によって保証されているか
のフラグ(YESまたはNO)、303は、フラグ302
に相当する電子署名を施した検証者の名前、304
は、対応する機能グループの実行を許可するか
のフラグ(OKまたはNOTOK)である。

【0022】図4は、本実施形態の処理を示すフローチ
ャートである。以下、図4に従い、本実施形態の詳細を
説明する。最初に、プログラム201の作成者が、
プログラム開発装置101上でプログラム201を作成する
(ステップ401)。

【0023】次に、プログラム201はコピーされて、
プログラム実行システム105～107に転送される
(ステップ402)。

【0024】転送は、オンラインシステム109を使用
しても使用しなくても良い。

【0025】次に、実行システム105～107の使用者（検証者）によって、プログラム201が実行され、その動作が危険なものでないかどうかを検証する（ステップ403）。

【0026】各検証は、各検証者ごとの機能グループに対して行われる。また、仕様書やソースプログラムコードの検証なども行われる。

【0027】ステップ403の処理の結果、検証対象とした機能グループが危険な動作をしないこと確認された時点で、電子署名装置102～104によって電子署名が施される（ステップ404）。

【0028】検証者の名前、ステップ404の電子署名の結果の電子署名データ、および検証した機能グループのIDがそれぞれ図2の202、203、204の欄に格納され、補助記憶装置101に記憶される（ステップ405）。

【0029】検証の後、プログラム実行システム108からプログラム201の送信を要求されたサーバシステム110は、図2の201～204のデータをプログラム実行システム108に対して送信する（ステップ406）。

【0030】プログラム実行システム108は、受信したデータを解析し、各電子署名データ203を確認し、図3に示したプログラム実行許可設定データを生成する（ステップ407）。

【0031】生成されたデータに対し、利用者がフラグ304を格納する。このとき、利用者は、検証者の名前303を参照し、この機能グループが危険な動作をしないということを信用するかどうかを判断する（ステップ408）。信用する場合は、フラグ304として「OK」を設定し、電子署名があったとしても信用できない場合は、「NOTOK」を設定する。

【0032】次にプログラム201は、プログラム実行システム108上で、フラグ304が「OK」になっている機能グループのみを実行する（ステップ409）。

【0033】このようにすることにより、1) プログラムの作成者は独立した検証者によって検証済みであることが分かるので、そのプログラムが危険な動作をしないことを直接証明することができる。

【0034】2) 多数のプログラムに対して、共通の検証者が電子署名を施すことにより、電子署名の確認とプログラムの実行許可の設定作業を簡略化し、また、信用できる検証者かどうかの検討を充分行うことが可能となる。

【0035】3) 利用者が必要としている機能グループについてのみ、危険な動作をしないことが保証されるため、一部危険な動作をすることが保証されていない機能グループがあったとしても、その実行を許可することができる。

【0036】第2の実施形態

図5は、本発明の第2の実施形態を示すシステム構成図である。

【0037】図5において、501は、適当なプログラムを実行する機能を持つ演算処理装置、502は、文字や図表を表示する機能を持つディスプレイ装置、503は、設定データを保存するための補助記憶装置、504は、補助記憶装置503に保存されている設定データに対し、電子署名を施す機能を持つ電子署名装置、505は、プログラムの転送に使用するオンラインシステム、506はオンライン経由でのプログラムの送信機能を持つサーバシステム、507はプログラムを保存する機能を持つ補助記憶装置である。

【0038】図6は、補助記憶装置503に保存されている設定データの構造を示している。

【0039】図6において、601は、演算処理装置501によって実行可能な機能のID番号、602～604はID番号601の各機能に対し入力されるパラメータである。任意のパラメータに対する設定である場合は「*」を格納する。605は、対応する機能601の実行を許可するか許可しないかを示すフラグである。

【0040】図7は、機能別の実行許可／不許可の設定画面例を示す図である。図7において、701は機能の詳細を表示する枠、702～704はこの機能に対し入力されたパラメータである。各パラメータは適当な入力装置を介して変更することができる。705は、この機能の実行を許可するか許可しないかを入力するメニューである。

【0041】図8は本実施形態の処理を示すフローチャートである。以下、図8に従い、本実施形態の詳細を説明する。まず、オンラインシステム505を介して、補助記憶装置507上に保存されているプログラムを、サーバシステム506から演算装置501に転送する（ステップ801）。次に、演算装置501上で、転送したプログラムを起動する。次に、補助記憶装置503に保存されている設定データが他者によって作成されたものである場合は、その電子署名を確認する（ステップ802、803）。そして、設定データの電子署名が正しいか、または自分自身が作成した設定データである場合は、それを演算装置501に読み出す（ステップ804）。

【0042】次に、プログラムの各機能をその内容に従い順に実行してゆく（ステップ807）。起動中に実行する各機能について、設定データの機能ID番号601に登録されている機能かどうかをチェックする（ステップ808）。

【0043】もし機能ID番号601に登録されており、かつ入力されたパラメータが602～604に登録されているものと一致しない場合は、図7に示した設定画面をディスプレイ装置502に表示する（ステップ809、810）。

【0044】すなわち、図7の701には、実行しようとした機能の詳細を表示し、702～704には実行時に入力されたパラメータを表示する。

【0045】実行者はこれらの情報を参照し、この機能の実行が不利益にならない場合は、メニュー705を「許可」に選択する（ステップ811、812）。

【0046】一方、この機能の実行が不利益になる場合は、メニュー705を「不許可」に設定する（ステップ814）。

【0047】この結果、図6の設定データの対応するI. 10 D番号601の欄が追加され、入力されたパラメータと、「許可／不許可」のフラグが格納される（ステップ813、815）。

【0048】ステップ809において、機能ID番号601および入力パラメータ602～604が一致した場合は、フラグ605に従ってその機能を実行するか、あるいは実行を中断する（ステップ817）。

【0049】また、任意の時点で、電子署名装置504を使用して、補助記憶装置503上の設定データに対し電子署名を施し、この設定データを別のプログラム実行システムの補助記憶装置に複写することで、同一の設定ファイルを利用することができる。

【0050】このようにすることにより、

1) 各プログラムに対し、実行可能な機能と不可能な機能とを実行者自身が選択することにより、実行者に対し不利益とならない範囲で最大限の機能を実行することができる。

【0051】2) 同一の実行環境にある複数のプログラム実行システムにおいて、実行の許可／不許可の設定を共有することにより、同一のプログラムを複数のプログラム実行システム上で効率よく実行することができる。

【0052】

【発明の効果】以上のように本発明によれば、オンラインでプログラムを受信後、そのプログラムを実行する機能を持つプログラム実行システムにおいて、次のような効果を得ることができる。

【0053】1) プログラムの作成者とは独立した検証者が検証していることが分かるため、そのプログラムが危険な動作をしないことを直接的に証明することができる。

【0054】2) 多数のプログラムに対して、共通の検証者が電子署名を施すことにより、電子署名の確認と

8 ログランの実行許可の設定作業を簡略化し、また、信用できる検証者かどうかの検討を充分行うことが可能となる。

【0055】3) 利用者が必要としている機能グループについてのみ、危険な動作をしないことが保証されるため、一部危険な動作をすることが保証されていない機能グループがあったとしても、その実行を許可することができる。

【0056】4) 各プログラムに対し、実行可能な機能と不可能な機能とを実行者自身が選択することにより、実行者に対し不利益とならない範囲で最大限の機能を実行することができる。

【0057】5) 同一の実行環境にある複数のプログラム実行システムにおいて、実行の許可／不許可の設定を共有することにより、同一のプログラムを複数のプログラム実行システム上で効率よく実行することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態のシステム構成図である。

【図2】第1の実施形態におけるプログラムの構造を示す図である。

【図3】第1の実施形態におけるプログラムの機能グループの実行許可設定データの構造図である。

【図4】第1の実施形態における処理を示すフローチャートである。

【図5】本発明の第2の実施形態のシステム構成図である。

【図6】第2の実施形態における設定データの構造図である。

【図7】第2の実施形態における実行の許可／不許可の設定画面例を示す図である。

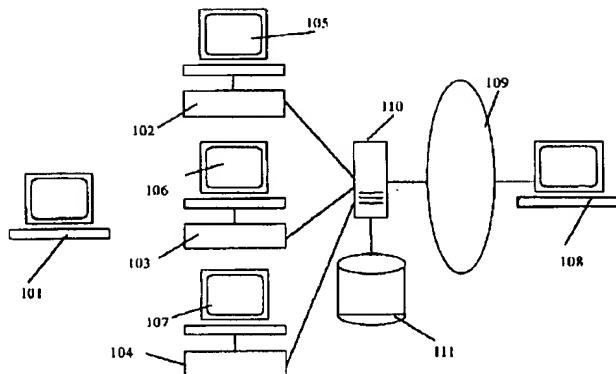
【図8】第2の実施形態における処理を示すフローチャートである。

【符号の説明】

101…プログラム開発装置、102～104…電子署名装置、105～108…プログラム実行システム、109…オンラインシステム、110…サーバシステム、111…補助記憶装置、501…演算処理装置、502…ディスプレイ装置、503…補助記憶装置、504…電子署名装置、505…オンラインシステム、506…サーバシステム、507…補助記憶装置。

【図1】

図1



【図2】

図2

201	プログラム	202	組織A	電子署名データA	204	FO01
		203	組織B	電子署名データB	205	FO02
		206	組織C	電子署名データC	207	FO03

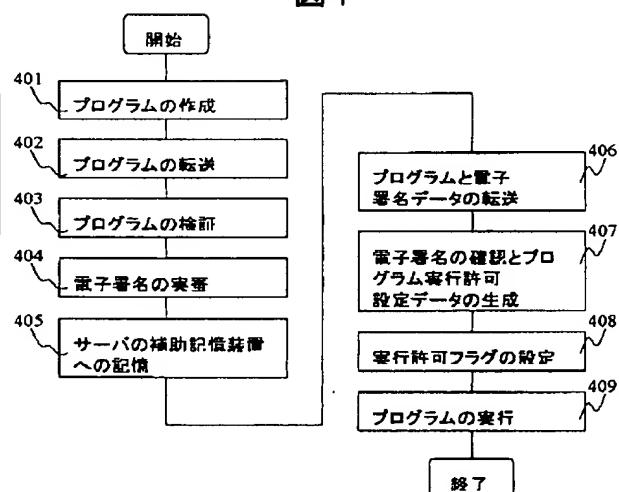
【図3】

図3

301	FO01	302	YES	303	組織A	304	OK
	FO02		NO		組織B		NOTOK
	FO03		YES		組織C		OK

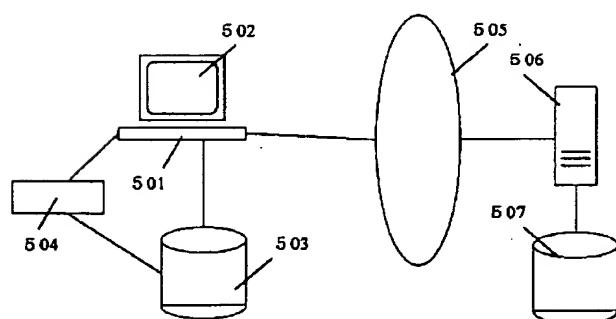
【図4】

図4



【図5】

図5



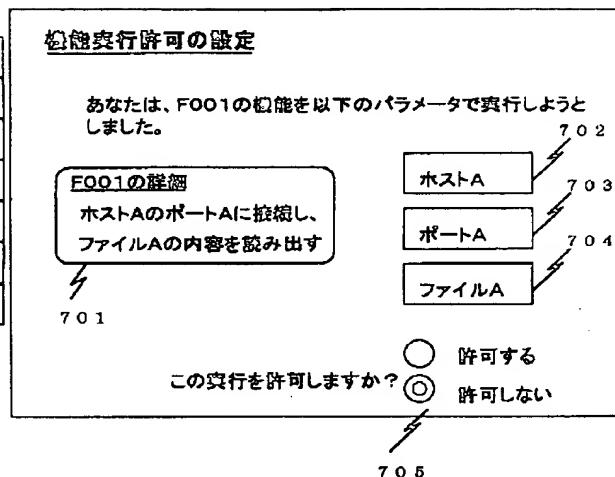
【図6】

図 6

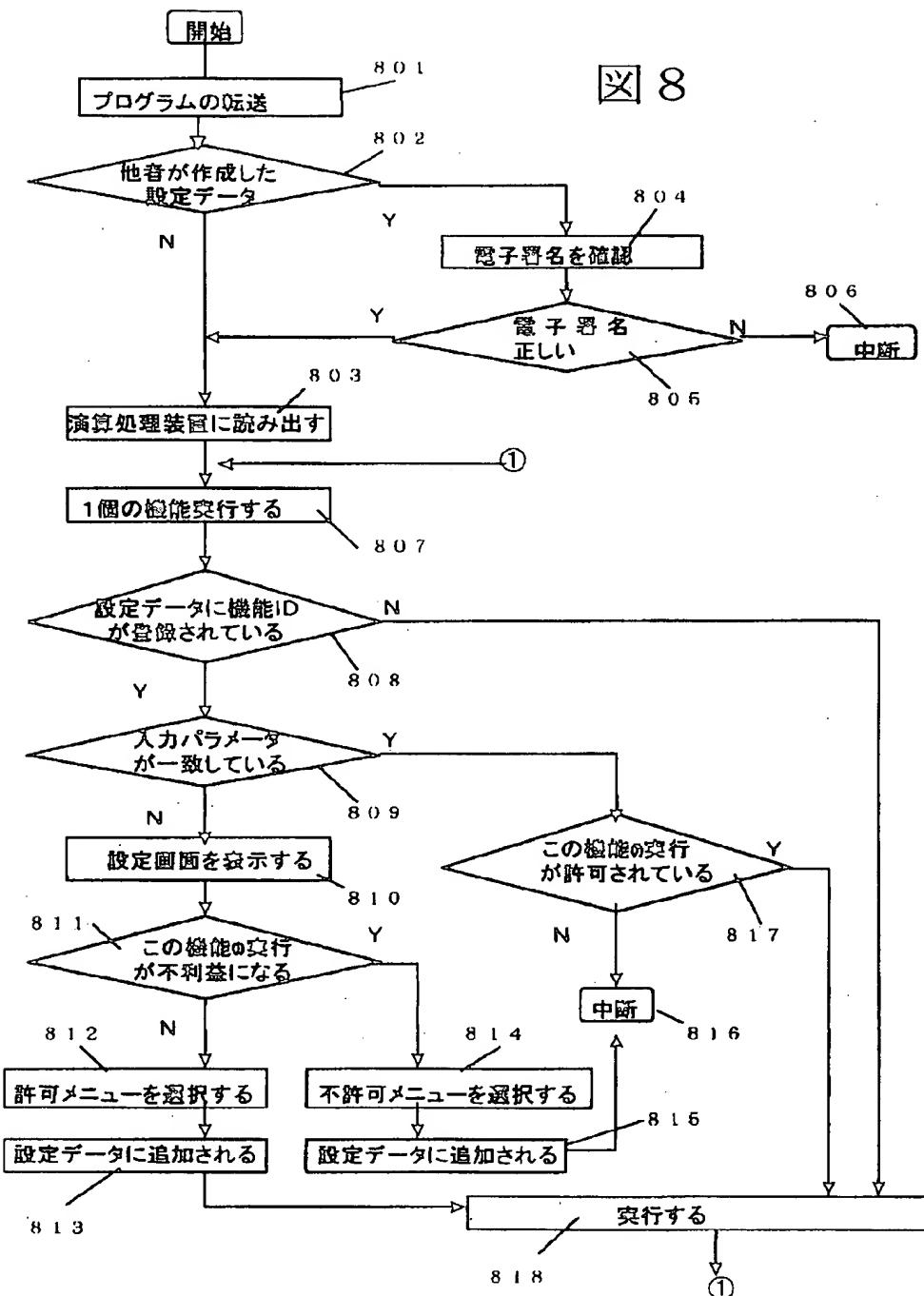
601	602	603	604	605
F001	ホストA	ポートA	ファイルA	OK
F001	ホストA	ポートB	ファイルB	OK
F001	ホストA	ポートC	*	NOTOK
F002	ファイルC	1024	"String"	OK
F003	ホストA	*	*	NOTOK
F003	ホストA	ファイルB	*	NOTOK
F003	ホストA	ファイルB	第N行	OK

【図7】

図 7



【図8】



8

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.